FYi

From the Information Policy Analysis Division

Volume 12 Issue 3
Summer 2013

FYi and Social Media 2.0:

Facebook, Twitter, YouTube, Yammer…and data practices?

Back in our fall 2009 FYi newsletter, IPAD wrote about emerging trends and options for government in using "social media" or "web 2.0." Since that time, government use of social media has grown (IPAD has since created a twitter account and a YouTube channel) and new social media options, such as Yammer, have emerged and evolved. As we've seen exponential social media growth in the last 4 years, we thought our readers would appreciate us sharing some of the questions and issues raised with IPAD since we addressed it in 2009.

As we wrote in 2009, remember that anything posted on a social media website is government data under the Government Data Practices Act (Minnesota Statutes, Chapter 13). Employees should only post public data when government is communicating via public websites such as Facebook and Twitter.

How long is an entity required to keep information posted on social media websites?

Entities should consider whether information communicated via social media are official records. If the communications are not official records, entities can decide how long to retain the information as government data. Data considered "official records" under the Official Records Act (Minnesota Statutes, section 15.17) must be kept according to an entity's retention schedule under the Records Management Act (Minnesota Statutes, section 138.17). For example, the general retention schedule for cities says correspondence through social media is to be retained "until read." If an entity posts an official record on a social media website (e.g. meeting minutes), an entity should consider keeping the official record in an alternative location. Visit Minnesota's State Archives website for more about records retention.

Are there any standards for how an entity should maintain data in a social media format?

Keep in mind the general standard for government data is they must be maintained in a format that's "easily accessible for convenient use" so that a government entity may respond to public data requests in an "appropriate and prompt manner" and within a "reasonable time." A good rule is to avoid archiving your data and you may want to have a plan for deleting data from a social media website at appropriate times.

Continued on page 2

Inside this issue:

Information Policy Analysis Division

Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Social media, cont.

yammer

The Enterprise Social Network

What is Yammer?

Yammer is advertised as “a private social network for your company.” Much like Facebook, users sign up and may create profiles, upload images or documents, and chat with other Yammer users online. Yammer allows users to create private groups that are invitation only. Tools like Yammer can be useful in collaborating within or outside your office.

If a government entity creates a private online group (e.g. private Yammer group that requires an invitation to join), is it subject to data requests from the public?

Yes, like any correspondence among government employees, all government data on any social media website are subject to the Data Practices Act. The general presumption, that all government data are public unless otherwise classified, applies.

Can an entity maintain or share private data on a private Yammer group that requires a password?

Generally, every entity has an obligation to establish appropriate safeguards to protect not public data and ensure that any access is related to a work requirement (see Minnesota Statutes, section 13.05, subd. 5 and Minnesota Rules, part 1205). Great care should be given before sharing not public data in any type of format. Government entities should consider the nature of the data and whether appropriate safeguards for sharing electronic data are in place, such as strong password protection and data encryption.

What if our website allows users to post public comments, should we provide any type of notice, such as a Tennessen warning?

Consider posting a notice that says the website is a public forum and users should refrain from posting questions or comments of a personal or private nature. A “Tennessen warning” is only required if an entity collects private or confidential data from an individual about the individual. Government entities should monitor comments submitted by the public and consider deleting posts that possibly contain private data or are inappropriate for a public forum.

As many government entities have learned since 2009, social media can be very useful in communicating and interacting with the public, or serve as an effective collaboration tool among government entities or within the office. If you know of a new social media tool, or have a question that we didn’t cover, contact us at info.ipad@state.mn.us ...and we may just revisit this topic again soon.

Advisory Opinion Highlights

Meetings Closed for Labor Negotiations

Opinion 13-012: A member of the public asked whether a city council had properly closed a meeting for labor negotiation strategies and developments pursuant to Minnesota Statutes, sections 13D.01 and 13D.03. The Commissioner opined that the City did not comply with section 13D.01, because it did not identify the authority to close the meeting or describe the subject of the meeting. The City did not comply with section 13D.03, because it failed to vote in open session to hold a closed meeting, as required, and because the Council also discussed subjects beyond the scope of labor negotiations and developments.

Law Enforcement Data on Driving Offenses

Opinion 13-013: A City asked about the classification of data on a driver's license magnetic stripe and driving citations that it wanted to collect, create, and maintain. The City argued that the data were public arrest data, pursuant to Minnesota Statutes, section 13.82, subd. 2. The Commissioner opined that the elements identified by the City as citation data were always public pursuant to section 13.82, subd. 2, for adult drivers. And, except for the name, sex, and address of adult drivers, which are public arrest data, the data on a driver's license magnetic stripe are presumptively public, unless the data are a part of an active investigation.

Caselaw Update

In ***Schwanke v. Minnesota Department of Administration*, A12-2062 (Minn. Ct. App. July 29, 2013),** the Minnesota Court of Appeals found that the Dept. of Admin did not have the statutory authority to dismiss a data challenge appeal of an employee's performance evaluation under Minnesota Statutes, section 13.04, subd. 4, and should have ordered a contested-case hearing with the Office of Administrative Hearings.

The Court held that Admin must order a contested case hearing unless efforts to resolve the dispute are successful. The Court looked to the Minnesota Administrative Procedures Act, Minnesota Statutes, Chapter 14, in determining that an Administrative Law Judge has exclusive authority to dismiss any unresolved data challenge. The Court also held that a data subject is allowed to submit new evidence to Admin, because a data challenge appeal is a de novo review, to be treated like a new hearing. *Note: Admin filed a petition for review with the MN Supreme Court on August 27, 2013.*

In ***National Council on Teacher Quality v. Minnesota State Colleges & Universities*, A12-2031 (Minn. Ct. App. August 5, 2013),** the Minnesota Court of Appeals affirmed the Ramsey County District Court's decision that MnSCU was required to provide copies of faculty-written syllabi to NCTQ under the Minnesota Government Data Practices Act, even though the syllabi are protected under federal copyright law. NCTQ, a national education-reform organization, requested copies of syllabi from MnSCU entities. MnSCU allowed NCTQ to inspect the syllabi, but declined to provide copies without the permission of the faculty authors, citing concern for their ownership rights.

Continued on page 4

Caselaw Update, cont.

The Court held that government entities may not assert copyright ownership to deny members of the public their right to inspect and copy government data, and that using copyright material for research is not an infringement of copyright, but is a “fair use” as asserted by NCTQ and defined under federal copyright law.

The Court of Appeals found in ***Computer Forensic v. Green*, A12-2093 (Minn. Ct. App. June 10, 2013, unpublished)**, that though a police detective likely released active investigation data (confidential data); the detective is entitled to official immunity for that action. The first step in determining official immunity is to find whether the conduct was ministerial or discretionary. The Court looked to the Minnesota Government Practices Act in finding it was discretionary: “Any law enforcement agency may make any data classified as confidential or protected nonpublic pursuant to subdivision 7 accessible to any person, agency, or the public if the agency determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.” (See Minnesota Statutes, section 13.82, subd. 15.) The detective and police department were entitled to official immunity because there was no evidence of willful or malicious intent (the second step in determining immunity) in this instance.

In ***Whalen v. Hennepin County Medical Center,* A13-0241 (Minn. Ct. App. July 15, 2013, unpublished)**, the Court of Appeals affirmed the District Court’s finding that a phone conversation between two employees was public data because it was the reason one of those employees was disciplined. Other than the data listed in Minnesota Statutes, section 13.43, subd. 2, personnel data are private; however, once there is a final disposition of a disciplinary action, “the specific reasons for the action and data documenting the basis of the action” are public (see section 13.43, subd. 2(a)(5)). HCMC made its final decision about discipline and there was final disposition, so the phone conversation documenting the reasons for that action is public.

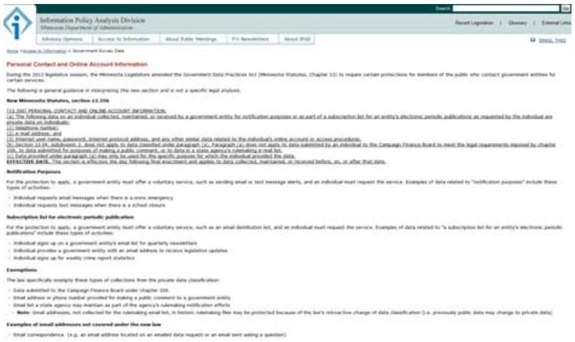
New IPAD Info Page!

Personal Contact and Online Account Information

During the 2013 legislative session, the Minnesota Legislature amended the Government Data Practices Act to require some protection for members of the public who contact government entities for certain services.

IPAD developed technical guidance to assist government and the public in understanding the implications of the new law.

http://www.ipad.state.mn.us/docs/personalcontact.html


Search
Go
Information Policy Analysis Division
Minnesota Department of Administration
Recent Legislation | Glossary | External Links
Advisory Opinions
Access to Information
About Public Meetings
FYI Newsletters
About IPAD
Email This
Home > Access to Information > Government Survey Data

Personal Contact and Online Account Information

During the 2013 legislative session, the Minnesota Legislature amended the Government Data Practices Act (Minnesota Statutes, Chapter 13) to require certain protections for members of the public who contact government entities for certain services.

The following is general guidance in interpreting this new section and is not a specific legal analysis.

New Minnesota Statutes, section 13.356

[13.356] PERSONAL CONTACT AND ONLINE ACCOUNT INFORMATION.
(a) The following data on an individual collected, maintained, or received by a government entity for notification purposes or as part of a subscription list for an entity's electronic periodic publications as requested by the individual are private data on individuals:
(1) telephone number;
(2) e-mail address; and
(3) Internet user name, password, Internet protocol address, and any other similar data related to the individual's online account or access procedures.
(b) Section 13.04, subdivision 2, does not apply to data classified under paragraph (a). Paragraph (a) does not apply to data submitted by an individual to the Campaign Finance Board to meet the legal requirements imposed by chapter 10A, to data submitted for purposes of making a public comment, or to data in a state agency's rulemaking e-mail list.
(c) Data provided under paragraph (a) may only be used for the specific purpose for which the individual provided the data.
EFFECTIVE DATE. This section is effective the day following final enactment and applies to data collected, maintained, or received before, on, or after that date.

Notification Purposes

For the protection to apply, a government entity must offer a voluntary service, such as sending email or text message alerts, and an individual must request the service. Examples of data related to "notification purposes" include these types of activities:

- Individual requests email messages when there is a snow emergency
- Individual requests text messages when there is a school closure

Subscription list for electronic periodic publication

For the protection to apply, a government entity must offer a voluntary service, such as an email distribution list, and an individual must request the service. Examples of data related to "a subscription list for an entity's electronic periodic publications" include these types of activities:

- Individual signs up on a government entity's email list for quarterly newsletters
- Individual provides a government entity with an email address to receive legislative updates
- Individual signs up for weekly crime report statistics

Exemptions

The law specifically exempts these types of collections from the private data classification:

- Data submitted to the Campaign Finance Board under chapter 10A
- Email address or phone number provided for making a public comment to a government entity
- Email list a state agency may maintain as part of the agency's rulemaking notification efforts
  - **Note**: Email addresses, not collected for the rulemaking email list, in historic rulemaking files may be protected because of the law's retroactive change of data classification (i.e. previously public data may change to private data).

Examples of email addresses not covered under the new law

- Email correspondence (e.g. an email address located on an emailed data request or an email sent asking a question)